- ABSTRACT -

Experience with Formal Methods Techniques at the Jet Prepulsion Laboratory from a Quality Assurance Perspective

By: John C. Kelly, Ph.D. and Rick Covington, Ph.D.
Software Product Assurance Section
Jet Prepulsion Laboratory
Pasadena, California, 91109

Over the past year and a half, a group of quality assurance personnel from the Jet Prepulsion Laboratory (JPL) has investigated the application of Formal Methods (FM) to several JPL projects, JPL's interest in FM has grown out of its need to develop hardware and software systems for its spacecraft under requirements that specify unusually high levels of reliability. Although traditionally considered too costly for large-scale application in industry, FM have more recently emerged as a practical technique for the assurance of increasingly complex system designs. This paper describes experience at JPL with FM applied to several pilot projects. We feel that FM shows promise for industry applications, especially in the area of high reliability systems, and we offer some concrete suggestions on how to integrate FM into the systems assurance process.

Previous studies of quality assurance activities at JPL have shown the software quality problem is greatest during the early lifecycle phases of requirements and design. These studies found

- The highest density of major defects found through the use of software inspections was during the requirements phase (an average of 1 major defect found per 3 pages of requirements documentation). This was 7 times higher than the density of major defects found in code inspections.

- Most hazardous software safety errors found during system integration and test of two NASA spacecraft were the result of requirements discrepancies or interface specifications.

Such results have motivated an interest in finding techniques for assuring the quality of engineering products in the earliest lifecycle possible.

FM, a set of techniques based on formal logical and mathematical reasoning, has been chosen as the focus of this investigation because of its promise for uncovering classes of specification and design errors which are not detectable by traditional means until much later lifecycle phases. FM is also believed to hold the potential for automation and systematization of many quality assurance activities which traditionally have been done manually and only on a small scale. Although the research community has investigated FM for more than a decade, FM has suffered

historically from the perception that it is not yet a sufficiently mature technique for full transition to industry, that it is only a collection of tools and not a thoroughly defined process which can be smooth] y integrated with an existing development processes. It is true that much early research into FM focused cm the application of FM to late lifecycle products such as source code, and the size of the product which could be analyzed by this technique was limited.

However, in response to the increasing focus on assurance activities in the early lifecycle, FM has been gradually refined and tailored to address problems such as requirements specification, where it has been successfully applied to problems of realistic size and complexity. To explore the applicability of FM to]1'1, systems development, the]1'1, working group identified several systems to serve as pilot projects. These systems included:

1. The Attitude and Articulation Control System (AACS) fault protection software for a spacecraft.
2. A detailed study of the floating point behavior of the 1750A Cl 'U to be used on spacecraf t flight computer boards
3. The Engine Gimbal Electronics (EGE) for a spacecraft.
4. The Deep Space Network (DSN) Block V Receiver Upgrade Task.

Based on these pilots, **]1'1,** experience supports the view that FM is ready for certain kinds of applications in industry. We describe concrete process steps which were evolved in the course of the]1'1, pilot studies to allow FM to be introduced into existing development and quality assurance processes, without the need to place FM analysis on any critical development path. We also report on an expansion of the FM idea to include high-level requirements simulators or "requirements animators". The use of animators facilitates a process in which quality assurance personnel provide FM expertise and development personnel provide application domain expertise. Animators then become a useful medium for communication of results of FM analysis between personnel who need the results but who need not be experts in FM. This experience suggests that quality assurance organizations could be a natural home for FM in many high reliability systems development environments.